

AO 106 (REV 4/10) Affidavit for Search Warrant

AUSA April M. Perry, (312) 886-5966

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION

FILED

FEB 13 2012

UNDER SEAL

MAGISTRATE JUDGE MARIA VALDEZ

UNITED STATES DISTRICT COURT

APPLICATION AND AFFIDAVIT
FOR SEARCH WARRANT

Case Number: **12 M 062**

In the Matter of the Search of:

The Facebook account associated with email address
ash2qt_1234@yahoo.com, further described in
Attachment A

I, Michael E. Brown, being duly sworn, depose and state that: I am a Special Agent of the Federal
Bureau of Investigation and have reason to believe that on the property or premises known as:

See Attachment A

in the Northern District of California there is now concealed certain property, namely:

DOCKETED

APR 30 2013

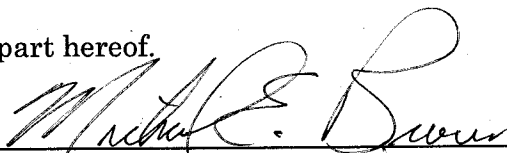
See Attachment A, Part III

which is evidence, concerning a violation of Title 18, United States Code, Section 242.

The facts to support a finding of probable cause are as follows:

See Attached Affidavit,

continued on the attached sheets and made a part hereof.



Signature of Affiant

MICHAEL E. BROWN

Special Agent, Federal Bureau of Investigation

Sworn to before me and subscribed in my presence,

February 13, 2012

Date

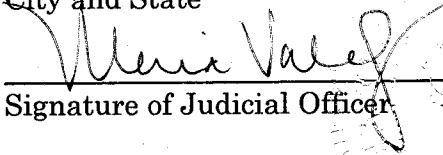
at

Chicago, Illinois

City and State

Maria Valdez, U.S. Magistrate Judge

Name & Title of Judicial Officer



Signature of Judicial Officer

UNITED STATES DISTRICT COURT)
) ss
NORTHERN DISTRICT OF ILLINOIS)

AFFIDAVIT

I, Michael E. Brown, being duly sworn, state as follows:

1. I am a Special Agent with the Federal Bureau of Investigation. I have been so employed since 1989.
2. As part of my duties as an FBI Special Agent, I investigate criminal violations involving corrupt public officials, including police officers. During my career, I have received training on and have investigated, among other things, civil rights offenses and violent crimes. I have participated in the execution of multiple federal search warrants.
3. This affidavit is made in support of an application for a warrant to search, pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), for information associated with an account that is stored at the premises owned, maintained, controlled, or operated by Facebook, a social network provider located at 1601 Willow Road, Menlo Park, CA 94025. The account to be searched is the Facebook account associated with email address ash2qt_1234@yahoo.com (hereinafter, "**Subject Account**"), which is further described in the following paragraphs and in Attachment A. As set forth below, there is probable cause to believe that in the account, described in Part II of Attachment A, in the

possession of Facebook, there exists evidence of a violation of Title 18, United States Code, Section 242.

4. The statements in this affidavit are based on my personal knowledge, and on information I have received from other law enforcement personnel and from persons with knowledge regarding relevant facts. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are sufficient to establish probable cause to believe that evidence of a violation of Title 18, United States Code, Section 242, is located in the **Subject Account**.

BACKGROUND INFORMATION

5. Based on my training and experience, and conversations with other law enforcement officers, I have learned the following about Facebook:

a. Facebook owns and operates a free-access social networking website of the same name that can be accessed at <http://www.facebook.com>. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

b. Facebook asks users to provide basic contact information to Facebook, either during the registration process or thereafter. This information

may include the user's full name, birth date, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook assigns a user identification number to each account.

c. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. A particular user's profile page also includes a "Wall," which is a space where the user and his or her "friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

d. Facebook users can access their accounts from any computer connected to the Internet located anywhere in the world.

e. Facebook uses the term "Neoprint" to describe an expanded view of a given user profile. The "Neoprint" for a given user can include the following information from the user's profile: profile contact information; Mini-Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers;

future and past event postings; rejected "friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications.

f. Facebook retains Internet Protocol ("IP") logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user's IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

g. In addition to storing information regarding the IP address from which a Facebook page is accessed, I have learned from other law enforcement agents and industry personnel that Facebook also may maintain records regarding which computer was used to access Facebook, and whether other Facebook users have used this same computer to access their Facebook accounts. This is known as records regarding associated users, machines, and cookies.

6. Therefore, the computers of Facebook are likely to contain all the material just described, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account

access information, transaction information, and account application. In order to accomplish the objective of the search warrant with a minimum of interference with the business activities of Facebook, to protect the rights of the subject of the investigation and to effectively pursue this investigation, authority is sought to allow Facebook to make a digital copy of the entire contents of the information subject to seizure specified in Section II of Attachment A. That copy will be provided to me or to any authorized federal agent. The contents will then be analyzed to identify records and information subject to seizure pursuant to Section III of Attachment A.

**FACTS SUPPORTING PROBABLE CAUSE
TO SEARCH THE SUBJECT ACCOUNT**

7. In or about April 2011, the Illinois State Police ("ISP") was investigating an allegation that Markham police officers had stolen money during the execution of a search warrant. During the course of the investigation, Officer A, a Markham police officer, agreed to cooperate with the ISP in hopes of being charged with a lesser offense in exchange for the information he provided and his cooperation with the ongoing investigation. To date, Officer A has not been charged. Officer A acknowledged that he and other officers stole money during the execution of the aforementioned search warrant. During the course of his cooperation, Officer A also informed the ISP that he had been

present when Officer B, another Markham police officer, had sexually assaulted a female in the custody of the Markham Police Department.

8. Specifically, Officer A informed law enforcement that in September 2010, Officer A was conducting an investigation into the sale and distribution of counterfeit currency. During the course of the investigation, Officer A and other officers conducted surveillance as a cooperating individual met with the supposed supplier of the counterfeit money. At the conclusion of the meeting, Officer A and other officers took into custody both the supposed supplier, as well as the woman ("Victim A") who had driven the supplier to the meeting. Officers seized \$5,000 in what they believed to be counterfeit currency from the supplier, and transported both the supplier and Victim A to the Markham Police Department.

9. Further according to Officer A, once the supposed supplier arrived at the station, Officer B questioned the supplier about the counterfeiting. Ultimately, Officer B asked the supplier what he planned to do to get out of trouble. When the supplier volunteered to pay Officer B, Officer B counted out \$4,500 of the \$5,000 in counterfeit currency and put it into Officer B's own pocket. Officer B then gave Officer A the remaining \$500, and told Officer A to place it into "Found Property." Officer A acknowledged that he took the money

and put it in his own locker. Officer A then placed the supplier in a holding cell at the Markham Police Department.

10. Officer A related that Officer B next asked about the female who had been arrested, and told Officer A to bring her to Officer B. Officer A then retrieved Victim A from a holding cell, and brought her to Officer B. Once Victim A arrived, Officer B began telling her that she was in trouble, and that she needed to do something to get herself out of trouble. According to Officer A, Victim A appeared scared, and asked Officer B what she needed to do. Officer B suggested that Victim A could do something to him to get out of trouble. Officer B then told her something to the effect of, "you know what to do with that mouth." Officer B told Officer A and another officer to stand guard by the door. Officer A left the room, but observed the room through a window in the door. Officer A observed as Victim A performed oral sex on Officer B, and then as Officer B and Victim A had sexual intercourse. Officer A then heard Officer B say he was "finished," and watched Officer B throw a used condom in a garbage can and tie up the garbage bag.

11. Following this, Officer A related that he and the other officer who had been outside the room re-entered the room. Officer B handed Officer A the garbage bag that contained the used condom, and told Officer A to get rid of it. Officer A thereafter placed the garbage bag into the dumpster outside the police

station. Officer A then related that Officer B told Victim A that she could use his computer, and he would eventually release her. Officer A observed as Victim A used Officer B's department-issued laptop computer. Ultimately, Officer B told Officer A to release Victim A. Officer A then walked Victim A out of the police station, where the supplier and an unknown individual were waiting.

12. After interviewing Officer A, ISP asked Officer A to provide to ISP the \$500 in counterfeit currency that Officer A claimed to have received from Officer B. On or about April 16, 2011, Officer A provided ISP with \$500 in what appeared to be counterfeit funds.

13. In approximately April 2011, ISP conducted an interview with Victim A. During this interview, Victim A acknowledged that she had been taken into custody by the Markham Police Department. When she was brought to Markham, Victim A stated that she was not booked or processed, nor told what she was charged with. Victim A was placed in a holding cell for approximately 30 minutes, and then was brought to the office of Officer B. Victim A related that Officer B began making sexual advances toward her, and that she was worried about having been arrested and her car possibly being impounded. After the other officers in the room left, Victim A stated that she performed oral sex on Officer B, and that he then had sexual intercourse with her. After Officer B ejaculated, Victim A stated that Officer B placed the condom into a garbage can.

Thereafter, the other officers came back, and Officer B told Victim A that she could check her Facebook account from Officer B's computer. Victim A spent some time on her Facebook page, and ultimately was allowed to leave the police station.

14. ISP officers showed Victim A a photo spread containing a photograph of Officer B. Victim A correctly identified Officer B from the photo spread.

15. In September 2011, ISP officers requested an offline search of a law enforcement database to obtain the names of subjects run by the Markham Police Department from September 17 through 24, 2010. The search revealed that on September 23, 2010, at approximately 4:37 p.m., the Markham Police Department conducted an inquiry on the name of the supposed counterfeit supplier. The search further revealed that on September 23, 2010, at approximately 4:39 p.m., the Markham Police Department conducted an inquiry on the name of Victim A.

16. In January 2012, I interviewed Victim A, who repeated the information she had provided to the ISP, to include the information concerning her accessing her Facebook page from Officer B's computer. Victim A further told me that the email address associated with her Facebook account was ash2qt_1234@yahoo.com.

SEARCH PROCEDURE

17. In order to facilitate seizure by law enforcement of the records and information described in Attachment A, this affidavit and application for search warrant seek authorization, pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), to permit employees of Facebook to assist agents in the execution of this warrant. In executing this warrant, the following procedures will be implemented:


- a. The search warrant will be presented to Facebook personnel who will be directed to the information described in Section II of Attachment A;
- b. In order to minimize any disruption of computer service to innocent third parties, Facebook employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the information described in Section II of Attachment A, including an exact duplicate of all information described in Section II of Attachment A;
- c. Facebook employees will provide the exact duplicate in electronic form of the information described in Section II of the Attachment A and all information stored in those accounts and files to the agent who serves this search warrant; and
- d. Following the protocol set out in the Addendum to Attachment A, law enforcement personnel will thereafter review all information and records

received from Facebook employees to locate the information to be seized by law enforcement personnel pursuant to Section III of Attachment A.

CONCLUSION

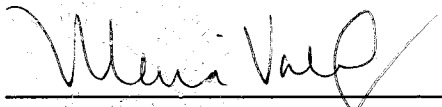
18. Based on the above information, I respectfully submit that there is probable cause to believe that evidence of a violation of Title 18, United States Code, Section 242 is located within one or more computers and/or servers found at Facebook, headquartered at 1601 Willow Road, Menlo Park, CA 94025. By this affidavit and application, I request that the Court issue a search warrant directed to Facebook allowing agents to seize the electronic evidence and other information stored on the Facebook servers following the search procedure described in Attachment A and the Addendum to Attachment A.

FURTHER AFFIANT SAYETH NOT.



Michael E. Brown
Special Agent
Federal Bureau of Investigation

Subscribed and sworn
before me this 13th day of February, 2012



Honorable Maria Valdez
United States Magistrate Judge

ATTACHMENT A

I. Search Procedure

1. The search warrant will be presented to Facebook personnel, who will be directed to isolate those accounts and files described in Section II below.

2. In order to minimize any disruption of computer service to innocent third parties, company employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the computer accounts and files described in Section II below, including an exact duplicate of all information stored in the computer accounts and files described therein.

3. Facebook employees will provide the exact duplicate in electronic form of the accounts and files described in Section II below and all information stored in those accounts and files to the agent who serves the search warrant.

4. Following the protocol set out in the Addendum to this Attachment, law enforcement personnel will thereafter review information and records received from company employees to locate the information to be seized by law enforcement personnel specified in Section III below.

II. Files and Accounts to be Copied by Facebook Employees

To the extent that the information described below is within the possession, custody, or control of Facebook, headquartered at 1601 Willow Road, Menlo Park, CA 94025, Facebook is required to disclose the following

information to the government for the account associated with email address ash2qt_1234@yahoo.com:

(a) All contact information for the account, including: full name, user identification number, birth date, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.

(b) All information about the user's login attempts and/or access and use of Facebook and Facebook applications in the month of September 2010.

(c) All communications and messages made or received by the user in September 2010, including all private messages and pending "Friend" requests;

(d) All IP logs, including all records of the IP addresses that logged into the account in September 2010.

(e) All common users, machines, and cookies associated with the account.

III. Information to be Seized by Law Enforcement Personnel

a. All information described above in Section II that constitutes evidence concerning violations of Title 18, United States Code, Section 242.

ADDENDUM TO ATTACHMENT A

With respect to the search of any information and records received from the social network provider, law enforcement personnel will locate the information to be seized pursuant to Section III of Attachment A according to the following protocol.

The search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein):

- a. searching for and attempting to recover any hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein.

- b. surveying various file directories and the electronic mail, including attachments thereto to determine whether they include data falling within the list of items to be seized as set forth herein.

- c. opening or reading portions of electronic mail, and attachments thereto, in order to determine whether their contents fall within the items to be seized as set forth herein, and/or

- d. performing key word searches through all electronic mail and attachments thereto, to determine whether occurrences of language contained

in such electronic mail, and attachments thereto, exist that are likely to appear in the information to be seized described in Section III of Attachment A.

Law enforcement personnel are not authorized to conduct additional searches on any information beyond the scope of the items to be seized by this warrant.